

JUDGE OETKEN

13 CIV 6919

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

Plaintiff,

- v. -

ROSS WILLIAM ULBRICHT,
a/k/a "Dread Pirate Roberts,"
a/k/a "DPR,"
a/k/a "Silk Road,"

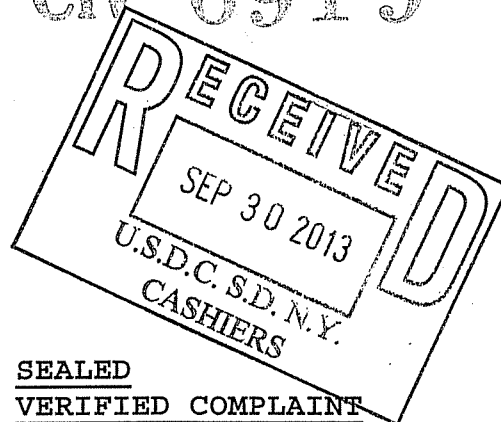
Defendant,

ANY AND ALL ASSETS OF SILK ROAD,
INCLUDING BUT NOT LIMITED TO THE
SILK ROAD HIDDEN WEBSITE AND ANY
AND ALL BITCOINS CONTAINED IN
WALLET FILES RESIDING ON SILK ROAD
SERVERS, INCLUDING THE SERVERS
ASSIGNED THE FOLLOWING INTERNET
PROTOCOL ADDRESSES:

46.183.219.244; 109.163.234.40;
193.107.86.34; 193.107.86.49;
207.106.6.25; AND 207.106.6.32;

And all property traceable
thereto,

Defendants-in-rem.



13 Civ.

Plaintiff United States of America, by its attorney, Preet
Bharara, United States Attorney for the Southern District of New
York, for its verified complaint alleges, upon information and
belief, as follows:

JURISDICTION AND VENUE

1. This action is brought by the United States of America pursuant to Title 18, United States Code, Section 981(a)(1)(A), seeking the forfeiture of ANY AND ALL ASSETS OF SILK ROAD, INCLUDING BUT NOT LIMITED TO:

- a. THE SILK ROAD HIDDEN WEBSITE;
- b. ANY AND ALL BITCOINS CONTAINED IN WALLET FILES RESIDING ON SILK ROAD SERVERS (the "DEFENDANT BITCOINS"), INCLUDING THE SERVERS ASSIGNED THE FOLLOWING INTERNET PROTOCOL ADDRESSES:
46.183.219.244; 109.163.234.40; 193.107.86.34;
193.107.86.49; 207.106.6.25; AND 207.106.6.32;

and all property traceable thereto (collectively the "Defendants in Rem").

2. The Government also seeks civil money laundering penalties against ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road," (the "Defendant in Personam") in an amount to be determined at trial.

3. This Court has jurisdiction over this action pursuant to Title 28, United States Code, Section 1355(b)(1), which provides that a forfeiture action or proceeding may be brought in the district court for the district in which any of the acts or omissions giving rise to the forfeiture occurred.

4. Venue is proper pursuant to Title 28, United States Code, Section 1395(a) because the cause of action accrued in the Southern District of New York. Since November of 2011, law

enforcement agents participating in this investigation have made multiple individual undercover purchases of controlled substances from Silk Road vendors, including purchases made from, and substances shipped to, the Southern District of New York. The payments for these controlled substances were then involved in money laundering transactions through the SILK ROAD HIDDEN WEBSITE.

FACTUAL OVERVIEW

5. As detailed below, from in or about January 2011, up to and including September 2013, the SILK ROAD HIDDEN WEBSITE, a Defendant in Rem, has served as a sprawling black-market bazaar, where illegal drugs and other illicit goods and services have been regularly bought and sold by the site's users.

6. The SILK ROAD HIDDEN WEBSITE is designed to facilitate the illicit commerce hosted on the site by providing anonymity to its users, in at least two ways. First, the SILK ROAD HIDDEN WEBSITE operates on what is known as "The Onion Router" or "Tor" network ("Tor"), a part of the Internet designed to make it practically impossible to physically locate the computers hosting or accessing websites on the network. Second, all transactions on the SILK ROAD HIDDEN WEBSITE must be paid with "Bitcoins," an electronic currency designed to be as anonymous as cash.

7. Upon information and belief, the SILK ROAD HIDDEN WEBSITE has emerged as the most sophisticated and extensive criminal marketplace on the Internet today. The site has sought to make conducting illegal transactions on the Internet as easy and frictionless as shopping online at mainstream e-commerce websites. During its two-and-a-half years in operation, the SILK ROAD HIDDEN WEBSITE has been used by several thousand drug dealers and other unlawful vendors to distribute hundreds of kilograms of illegal drugs and other illicit goods and services to well over a hundred thousand buyers, and to launder hundreds of millions of dollars deriving from these unlawful transactions. All told, the site has generated sales revenue totaling over 9.5 million Bitcoins and collected commissions from these sales totaling over 600,000 Bitcoins. Although the value of Bitcoins has varied significantly during the site's lifetime, these figures are roughly equivalent today to approximately \$1.2 billion in sales and approximately \$80 million in commissions.

8. An individual named ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road," the Defendant in Personam, has overseen Silk Road's operation since its inception and has controlled the massive profits generated from the operation of the business. ULBRICHT has always been aware of the illegal nature of his enterprise. Throughout its

operation, he has sought to ensure the anonymity of the drug dealers and other illegal vendors operating on the site, as well as to conceal his own identity as the owner and operator of the site.

9. The illegal nature of the items sold on the SILK ROAD HIDDEN WEBSITE is readily apparent to any user browsing through its offerings. The vast majority of the goods for sale consist of illegal drugs of nearly every variety, which are openly advertised on the site as such, and are immediately and prominently visible on the site's home page.

10. As of September 20, 2013, there were nearly 13,000 listings for controlled substances on the SILK ROAD HIDDEN WEBSITE, listed under the categories "Cannabis," "Dissociatives," "Ecstasy," "Intoxicants," "Opioids," "Precursors," "Prescription," "Psychedelics," and "Stimulants," among others.

11. The narcotics sold on the site tend to be sold in individual-use quantities, although some vendors sell in bulk. The offerings for sale on the site at any single time amount to multi-kilogram quantities of heroin, cocaine, and methamphetamine, as well as distribution quantities of other controlled substances, such as LSD.

12. Besides illegal narcotics, other black-market goods and services -- such as computer-hacking services and fake

identity documents -- are openly advertised and sold on the SILK ROAD HIDDEN WEBSITE as well.

13. Not only are the goods and services offered on the SILK ROAD HIDDEN WEBSITE overwhelmingly illegal on their face, but the illicit nature of the commerce conducted through the website is openly recognized in the Silk Road online community. For example, information available on the SILK ROAD HIDDEN WEBSITE provides extensive guidance to users concerning how to conduct transactions on the site without being caught by law enforcement.

14. Silk Road charges a commission for every transaction conducted by its users. The commission rate varies, generally between 8 to 15 percent, depending on the size of the sale, *i.e.*, the larger the sale, the lower the commission.

15. Since November of 2011, law enforcement agents participating in this investigation have made over 100 individual undercover purchases of controlled substances from Silk Road vendors, including purchases made from, and substances shipped to, the Southern District of New York. The substances purchased in these undercover transactions have been various Schedule I and II drugs, including ecstasy, cocaine, heroin, LSD, and others. Samples of these purchases have been laboratory-tested and have typically shown high purity levels of the drug the item was advertised to be on the SILK ROAD HIDDEN

WEBSITE. Based on the postal markings on the packages in which the drugs arrived, these purchases appear to have been filled by vendors located in over ten different countries, including the United States, Germany, the Netherlands, the United Kingdom, Spain, Canada, Ireland, Italy, Austria and France. Agents have also made undercover purchases of hacking services on the SILK ROAD HIDDEN WEBSITE, including purchases of malicious software such as remote access tools ("RATs") that allow a hacker to remotely control and steal information from infected computers.

THE RELATED CRIMINAL CASE

16. On or about September 27, 2013, the Honorable Frank Maas, United States Magistrate Judge, signed a sealed criminal complaint charging ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road," the Defendant in Personam, with conspiracy to violate the narcotics laws of the United States, in violation of Title 21, United States Code, Section 846 (the "Narcotics Offense"); with conspiracy to commit computer intrusion offenses in violation of Title 18, United States Code, Section 1030(a)(2) (the "Computer Hacking Offense"); and with conspiracy to commit money laundering in violation of Title 18, United States Code, Section 1956(h). See *United States v. Ross William Ulbricht*, 13 Mag. 2328 (FM) (the "Criminal Complaint").

- a. The Criminal Complaint alleges, among other things, that ULBRICHT engaged in a conspiracy to distribute controlled substances in violation of Title 21, United States Code, Section 841(a)(1), and to distribute controlled substances by means of the Internet, in a manner not authorized by law, in violation of Title 21, United States Code, Section 841(h), by owning and operating the Silk Road website, which has provided a platform for drug dealers around the world to sell a wide variety of controlled substances via the Internet.
- b. The Criminal Complaint further alleges, among other things, that ULBRICHT engaged in a conspiracy to access computers without authorization in order to obtain information for purposes of financial gain, in violation of Title 18, United States Code, Section 1030(a)(2).
- c. The Criminal Complaint further alleges, among other things, that ULBRICHT engaged in a conspiracy to conduct financial transactions involving the proceeds of the Narcotics Offense and the Computer Hacking Offense, with the intent to promote the carrying on of such specified unlawful activity and knowing that the transactions were designed to conceal and disguise the nature, the location, the source, the ownership, and the control of the proceeds of specified unlawful activity, in violation of Title 18, United States Code, Sections 1956(a)(1)(A)(i) and 1956(a)(1)(B)(i).

17. A true and correct copy of the Criminal Complaint is attached hereto as Exhibit A and is incorporated by reference as if fully set forth herein.

SILK ROAD'S HIDDEN WEBSITE

18. As noted above and as alleged in the Criminal Complaint, the SILK ROAD HIDDEN WEBSITE, a Defendant in Rem, operates on the Tor network. Tor enables websites like the SILK

ROAD HIDDEN WEBSITE to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites. Such "hidden services" operating on Tor have complex pseudo-domain names, generated by a computer algorithm, ending in ".onion." For example, the pseudo-domain name for the SILK ROAD HIDDEN WEBSITE is currently "silkroadvb5piz3r.onion." Websites with such ".onion" pseudo-domain names can be accessed only by using Tor browser software. However, such software can be easily downloaded for free on the Internet.

19. In order to access the SILK ROAD HIDDEN WEBSITE, a user need only download Tor browser software onto his or her computer, and then type in Silk Road's ".onion" pseudo-domain name into the user's Tor browser. Silk Road's ".onion" pseudo-domain name can be found in various online forums and other websites on the ordinary Internet.

20. The Tor network uses a particular protocol to direct traffic to each hidden service on that network. In particular, every ".onion" pseudo-domain name has a corresponding unique "key," consisting of letters, numbers and symbols. The key, which may be stored on any server on the Tor network, serves to authenticate the validity of the ".onion" pseudo-domain name. Typically, certain servers on the Tor network ("traffic servers") function to match each ".onion" pseudo-domain name - as authenticated by the key - to the physical server on which

the hidden website is hosted. Typically, when a user wants to access a hidden service, the user types the associated ".onion" pseudo-domain name into his or her Tor browser. The browser software then checks with the traffic servers on the Tor network, which direct the user to the appropriate ".onion" server and, in turn, the server on which the associated hidden service is hosted. Accordingly, both the ".onion" pseudo-domain name and corresponding key are required to exercise control over a particular hidden service on the Tor network.

21. Upon information and belief, the United States has not only learned the current and publicly available ".onion" pseudo-domain name for the SILK ROAD HIDDEN WEBSITE ("silkroadvb5piz3r.onion"), but has also located a server containing the corresponding authentication key and has obtained a copy of that key.

BITCOINS IN GENERAL

22. Bitcoins are an anonymous, decentralized form of electronic currency, existing entirely on the Internet and not in any physical form. The currency is not issued by any government, bank, or company, but rather is generated and controlled automatically through computer software operating on a "peer-to-peer" network. Bitcoin transactions are processed collectively by the computers composing the network.

23. In order to acquire Bitcoins in the first instance, a user typically must purchase them from a Bitcoin "exchanger." In return for a commission, Bitcoin exchangers accept payments of currency in some conventional form (cash, wire transfer, etc.) and exchange the money for a corresponding amount of Bitcoins, based on a fluctuating exchange rate. Conversely, exchangers also accept payments of Bitcoins and exchange the Bitcoins back for conventional currency, again, charging a commission for the service.

24. Once a user acquires Bitcoins from an exchanger, the Bitcoins are kept in a "wallet" associated with a Bitcoin "address," designated by a complex string of letters and numbers. (The "address" is analogous to the account number for a bank account, while the "wallet" is analogous to a bank safe where the money in the account is physically stored.) Once a Bitcoin user funds his wallet, the user can then use Bitcoins in the wallet to conduct financial transactions, by transferring Bitcoins, over the Internet, from his Bitcoin address to the Bitcoin address of another user.

25. All Bitcoin transactions are recorded on a public ledger known as the "Blockchain," which exists in order to prevent a user from spending the same Bitcoins more than once. However, the Blockchain only reflects the movement of funds between anonymous Bitcoin addresses and therefore cannot by

itself be used to determine the identities of the persons involved in the transactions. Only if one knows the identities associated with each Bitcoin address involved in a set of transactions is it possible to meaningfully trace funds through the system.

26. Bitcoins are not illegal in and of themselves and have known legitimate uses. However, Bitcoins are also known to be used by cybercriminals for money-laundering purposes, given the ease with which they can be used to move money anonymously.

SILK ROAD'S BITCOIN-BASED PAYMENT SYSTEM

27. The only form of payment accepted on the SILK ROAD HIDDEN WEBSITE is Bitcoin. Every user on the SILK ROAD HIDDEN WEBSITE has a Silk Road Bitcoin address, or multiple addresses, associated with the user's Silk Road account. These addresses are stored on wallets maintained on servers controlled by Silk Road.

28. Silk Road's payment system essentially consists of a Bitcoin "bank" internal to the site, where every user must hold an account in order to conduct transactions on the site. Specifically, in order to make purchases on the SILK ROAD HIDDEN WEBSITE, the user must first obtain Bitcoins (typically from a Bitcoin exchanger) and send them to a Bitcoin address associated with the user's Silk Road account. After thus funding his or her account, the user can then make purchases from Silk Road

vendors. When the user purchases an item on the SILK ROAD HIDDEN WEBSITE, the Bitcoins needed for the purchase are held in escrow (in a wallet maintained by Silk Road) pending completion of the transaction. Once the transaction is complete, the user's Bitcoins are transferred to the Silk Road Bitcoin address of the vendor involved in the transaction. The vendor can then withdraw Bitcoins from Silk Road by sending them to a different Bitcoin address, such as the address of a Bitcoin exchanger who can cash out the Bitcoins for real currency.

29. The computer code used to run the SILK ROAD HIDDEN WEBSITE reflects the use of certain Bitcoin wallets (the "Silk Road wallets"), which contain user funds in the form of Bitcoins on deposit with Silk Road, namely, the DEFENDANT BITCOINS. The balances in these Silk Road wallets (obtained from another Silk Road-associated server) generally show millions of dollars' worth of DEFENDANT BITCOINS on deposit with Silk Road on a regular basis. The following is a sample of the balances contained in the Silk Road wallets over a two-day time period:

<u>Date/Time</u>	<u>Total Bitcoins</u>	<u>Approx. USD</u>
9/14/2013 6:00 UTC	18205.50649	\$2,548,770.91
9/14/2013 12:00 UTC	17420.92877	\$2,438,930.03
9/14/2013 18:00 UTC	17088.67959	\$2,358,237.79
9/15/2013 0:00 UTC	13950.06159	\$1,911,158.44
9/15/2013 6:00 UTC	16143.52567	\$2,195,519.49

9/15/2013 12:00 UTC	15955.46307	\$2,217,809.37
9/15/2013 18:00 UTC	16069.43546	\$2,233,651.53

30. Based upon statements made by ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road," the Defendant in Personam, these Silk Road wallets are believed to be under the exclusive control of ULBRICHT, as owner and operator of the SILK ROAD HIDDEN WEBSITE. Although ULBRICHT is known to delegate certain administrative functions regarding the operation of the SILK ROAD HIDDEN WEBSITE to his subordinates, the investigation has revealed that ULBRICHT does not similarly share access to the Silk Road wallets with anyone. The username and password that allow ULBRICHT to control the Silk Road wallets are stored on servers to which it is believed that only ULBRICHT has access.

31. The investigation has revealed that some of the Silk Road wallets used by ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road," the Defendant in Personam, to operate the SILK ROAD HIDDEN WEBSITE may be located on computer servers assigned the following IP addresses¹:

a. 46.183.219.244;

¹ Every computer device on the Internet has an Internet protocol or "IP" address assigned to it, which is used to route Internet traffic to or from the device.

- b. 109.163.234.40;
- c. 193.107.86.34;
- d. 193.107.86.49;
- e. 207.106.6.25; and
- f. 207.106.6.32.

PROBABLE CAUSE FOR FORFEITURE

32. As explained above and as alleged in the Complaint, ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road," the Defendant in Personam, through his ownership and operation of the SILK ROAD HIDDEN WEBSITE, engaged in a money-laundering conspiracy by operating an online marketplace that was designed to facilitate anonymous and untraceable transactions involving illicit goods and services.

33. The Silk Road wallets are an essential component of the Silk Road system, as they contain all user funds on deposit with Silk Road, in the form of the DEFENDANT BITCOINS, and thus compose the "operating account" of the business.

34. Accordingly, the Defendants in Rem - including the SILK ROAD HIDDEN WEBSITE and the DEFENDANT BITCOINS - are property involved in the money laundering conspiracy charged in the Criminal Complaint, and are subject to forfeiture to the United States under Title 18, United States Code, Section 981(a)(1)(A).

35. In sum, there is probable cause to believe that the Defendants in Rem constitute property involved in a conspiracy to commit money laundering, or property traceable to such property, in violation of Title 18, United States Code, Section 1956(h). Accordingly, the Defendants in Rem are subject to forfeiture to the United States of America pursuant to Title 18, United States Code, Section 981(a)(1)(A).

FIRST CLAIM
(FORFEITURE UNDER 18 U.S.C. §§ 981(a)(1)(A))

36. Paragraphs 1 through 35 of this Complaint are repeated and realleged as if fully set forth herein.

37. Pursuant to Title 18, United States Code, Section § 981(a)(1)(A), "[a]ny property, real or personal, involved in a transaction in violation of section 1956 [or] 1960 . . . of [Title 18], or any property traceable to such property," is subject to forfeiture.

38. Pursuant to Title 18, United States Code, Section 1956, commonly known as the "money laundering" statute, a person who:

(a)(1) . . . knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity -

(A) (i) with the intent to promote the carrying on of specified unlawful activity; or

(ii) with intent to engage in conduct constituting a violation of section 7201 or 7206 of the Internal Revenue Code of 1986; or

(B) knowing that the transaction is designed in whole or in part -

(i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity; or

(ii) to avoid a transaction reporting requirement under State or Federal law,

shall be guilty of a crime.

39. Title 18, United States Code, Section 1956(h) further provides that "[a]ny person who conspires to commit any offense defined in this section or section 1957 shall be subject to the same penalties as those prescribed for the offense the commission of which was the object of the conspiracy."

40. For purposes of Sections 1956, "specified unlawful activity" includes, among other things, the Narcotics Offense and the Computer Hacking Offense.

41. By reason of the above, the Defendants In Rem are subject to forfeiture pursuant to Title 18, United States Code, Section 981(a)(1)(A).

SECOND CLAIM
(CIVIL MONEY LAUNDERING PENALTIES,
18 U.S.C. §§ 1956(a)(1)(A) and (b))

42. Paragraphs 1 through 35 of this Complaint are repeated and realleged as if fully set forth herein.

43. Pursuant to Title 18, United States Code, Section 1956(b), "[w]hoever conducts or attempts to conduct a transaction described in subsection (a)(1) or (a)(3), or section 1957, or a transportation, transmission, or transfer described in subsection (a)(2), is liable to the United States for a civil penalty of not more than the greater of - (A) the value of the property, funds, or monetary instruments involved in the transaction; or (B) \$10,000."

44. The Defendant in Personam engaged in financial transactions involving the proceeds of the Narcotics Offense and the Computer Hacking Offense, and therefore involving specified unlawful activity within the meaning of the money laundering statute.

45. The Defendant in Personam acted with the intent to promote the carrying on of the Narcotics Offense and the Computer Hacking Offense.

46. Accordingly, the Defendant in Personam is liable to the United States for the value of the funds and monetary instruments involved in the transactions, in an amount to be determined at trial.

THIRD CLAIM
(CIVIL MONEY LAUNDERING PENALTIES,
18 U.S.C. §§ 1956(a)(1)(B) and (b))

47. Paragraphs 1 through 35 of this Complaint are repeated and realleged as if fully set forth herein.

48. The Defendant in Personam engaged in financial transactions involving the proceeds of the Narcotics Offense and Computer Hacking Offense, and therefore involving specified unlawful activity within the meaning of the money laundering statute.

49. The Defendant in Personam knew that the financial transactions were designed in whole or in part to conceal or disguise the nature, location, source, ownership, or control of the proceeds of the Narcotics Offense and the Computer Hacking Offense.

50. Accordingly, the Defendant in Personam is liable to the United States for the value of the funds and monetary instruments involved in the transactions, in an amount to be determined at trial.

REQUEST FOR RELIEF

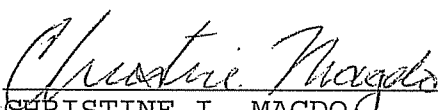
WHEREFORE plaintiff, the United States of America, requests that judgment be entered as follows:

- a. Enter judgment against the Defendants in Rem, and in favor of the United States, on the first claim alleged in the Complaint.

- b. Issue process to enforce the forfeiture of the Defendants in Rem, requiring that all persons having an interest in the Defendants in Rem be cited to appear and show cause why the forfeiture should not be decreed, and that this Court decree forfeiture of the Defendants in Rem to the United States of America for disposition according to law.
- c. Enter judgment against the Defendant in Personam, and in favor of the United States, on the second and third claims alleged in the Complaint.
- d. Award the United States civil money laundering penalties from the Defendant in Personam on the second and third claims alleged in the Complaint, in an amount to be proven at trial to a jury, plus prejudgment and postjudgment interest.
- e. Grant the Government such further relief as this Court may deem just and proper, together with the costs and disbursements in this action.

Dated: September 30, 2013
New York, New York

PREET BHARARA
United States Attorney for the
Southern District of New York

By: 
CHRISTINE I. MAGDO
Assistant United States Attorneys
One Saint Andrew's Plaza
New York, New York 10007
Tel.: (212) 637-2297
Facsimile: (212) 637-0421

VERIFICATION

STATE OF NEW YORK)
COUNTY OF NEW YORK)
SOUTHERN DISTRICT OF NEW YORK)

Gary L. Alford, being duly sworn, deposes and says that he is a Special Agent with the United States Internal Revenue Service - Criminal Investigation, and, as such, has responsibility for the within action; that he has read the foregoing complaint and knows the contents thereof, and that the same is true to the best of his own knowledge, information, and belief.

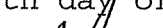
The sources of the deponent's information and the grounds for his belief are his personal knowledge and the official records and files of the United States Government.

Dated: New York, New York
September 30, 2013

Gary L. Alford
Special Agent
Internal Revenue Service -
Criminal Investigation

Sworn to before me this
30th day of September, 2013

30th day of September, 2011



Notary Public

MARCO DASILVA
Notary Public, State of New York
No. 01DA6145603
Qualified in Nassau County
My Commission Expires May 8, 2014